UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/021,042	12/19/2001	Masahiro Kaminaga	HITA.0144	6164

38327 7590 05/18/2005

REED SMITH LLP
3110 FAIRVIEW PARK DRIVE, SUITE 1400
FALLS CHURCH, VA 22042

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/021,042	KAMINAGA ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 16-20* is/are rejected.

7)☒ Claim(s) *5-15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3 AND 4/*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-19** have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Specification

3. The disclosure is objected because of the following informalities:

- On page 13, lines 15-18, the following mathematical expression is recited

  S = C [0] * C [1] * * C [511] mod N

  = (y ^(x [0] * 4 ^511)) * (y ^ (**x [0]** * 4 ^510)) *... * (y **x [0]**) mod N

  = y ^ (x [0] * 4 ^511 + x [1] * 4 ^510 +... + x [511]) mod N

  = y ^x mod N

  It has to be corrected as the follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

  S = C [0] * C [1] * * C [511] mod N

  = (y ^(x [0] * 4 ^511)) * (y ^ (**x [1]** * 4 ^510)) *... * (y ^ **x [511]**) mod N

  = y ^ (x [0] * 4 ^511 + x [1] * 4 ^510 +... + x [511]) mod N

  = y ^x mod N

- Page 19, line 9-10, the following has been recited. "Hereinafter, binary representation of k is written as (k[0]k[1]....k[79]), where **x[j]** is a 2-bit block that is equal to one of 00, 01, 10 and 11.

It has to be corrected as follows

- Page 19, line 9-10, the following has been recited. "Hereinafter, binary representation of k is written as (k[0]k[1]....k[79]), where **k[j]** is a 2-bit block that is equal to one of 00, 01, 10 and 11.

- On page 23, lines 9-14, the following mathematical expression is recited

"C[V(j)]=B[V(j)] x[V(j)] mod N (j=0, 1, 2, . . . , 511), upon termination of all processing, the following expression

S = C [V (0)] * C [V (1)] * * C [V (511)] mod N
= (y (x^ [V (0)] * 4 (511 - V (0))) * (y ^ (x [V (1)] * 4^ (512 - V (1))) *... *
(y^ (x [**V (0)**] * 4 ^ (511 - V (511))) mod N
= y ^ (x [V (0)] * 4^ (511 - V (0)) + x [V (1)] * 4 ^ (512 - V (1)) +...
+ x [**V (0)**] * 4 ^ (511 - V (511)) mod N"

The above mathematical expression has to be corrected as the follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

"S = C [V (0)] * C [V (1)] * * C [V (511)] mod N
= (y (x^ [V (0)] * 4 (511 - V (0))) * (y ^ (x [V (1)] * 4^ (512 - V (1))) *... *
(y^ (x [**V (511)**] * 4 ^ (511 - V (511))) mod N
= y ^ (x [V (0)] * 4^ (511 - V (0)) + x [V (1)] * 4 ^ (512 - V (1)) +...
+ x [**V (511)**] * 4 (511 - V (511)) mod N"

- On page 23, lines 17, the following mathematical expression is recited, "because of the nature of mapping V, since V(0), V(1), . . . , V(511) is an rearrangement of 0, 1, . . . , 511, the above described exponent part x[V(0)]*4^ (511-V(0))+x[V(1)]*4^ (512-V(1))+ . . . +x[**V(0)**]*4 ^ (511-V(511)) is equal to x[0]*4^ 511+x[1]*4^ 510+ . . . +x[511]."

  The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

  "because of the nature of mapping V, since V(0), V(1), . . . , V(511) is an rearrangement of 0, 1, . . . , 511, the above described exponent part x[V(0)]*4^ (511-V(0))+x[V(1)]*4^ (512-V(1))+ . . . +x[**V(511)**]*4 (511-V(511)) is equal to x[0]*4^ 511+x[1]*4 ^ 510+ . . . +x[511]."

- On page 25, on the first line, the following mathematical expression is recited, "V(j)=((7*(V(j)+1) mod 81) 1".
  It has to be corrected as follows,
  "V(j)=((7*(V(j)+1) mod 81) -1".

- On page 26, lines 5-8, the following mathematical expression is recited,
  "S = C [V (0)] + C [V (1)] + + C [V (511)]
  = (k [V (0)] * 4 (79 - V (0)) P + (k [V (1)] * 4 ^ (**512** - V (1)) P +... + (k [V (**0**)] * 4 ^ (**511** - V (**511**)) P
  = (k [V (0)] * 4 (79 - V (0)) + k [V (1)] * 4 (79 - V (1)) + + k [V (0)] * 4 (79 - V (79))) P"

  The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

"S = C [V (0)] + C [V (1)] + + C [V (511)]

= (k [V (0)] * 4 (79 - V (0)) P + (k [V (1)] * 4 ^ (**79** - V (1)) P +... + (k [V (**79**)] * 4 ^ (**79** - V (**79**)) P

= (k [V (0)] * 4^ (79 - V (0)) + k [V (1)] * 4^ (79 - V (1)) + + k [V (0)] * 4^ (79 - V (79))) P"

- On page 26, lines 11, the following mathematical expression is recited,

  k[V(0)]*4 ^ (79-V(0))+k[V(1)]*4 ^ (79-V(1))+ . . . +k[**V(0)**]*4^ (79-V^ (79)) is equal to k[0]*4 ^ 79+k[1]*4 ^ 78+ . . . +k[79].

  The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

  k[V(0)]*4 ^ (79-V(0))+k[V(1)]*4 ^ (79-V(1))+ . . . +k[**V(79)**]*4^ (79-V^ (79)) is equal to k[0]*4 ^ 79+k[1]*4 ^ 78+ . . . +k[79].

- On page 27, lines 3, the following mathematical expression is recited,

  (2 **m1**)P=(2 m)P+(-P).

  The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

  (2 **m-1**)P=(2 m)P+(-P).

- On page 27, lines 13, the following mathematical expression is recited,

  3=4 1

The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

3=4-1

- On page 27, lines 15, the following mathematical expression is recited,

195P=1*((4^ **4)P)(4 ^3)**P+0*((4^ 2)P)+1*4P-P.

The above mathematical expression has to be corrected as follows, otherwise the mathematical expression/equation of the two expression would not be equal and valid.

195P=1*((4^ **4)P)-(4 ^3)**P+0*((4^ 2)P)+1*4P-P.

Applicant is required to make the appropriate correction.

If there is other correction, that the examiner fails to point out, applicant is required to review the application and make the appropriate correction.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-4,16-20** are rejected under 35 U.S.C. 102(e) as being anticipated by Ohki et al. (hereinafter referred to as Ohki) (U.S. Patent No. 6,408,075).

6. **Claims 1-4,16-20** are rejected under 35 U.S.C. 102(b) as being anticipated by Kabushiki Kaisha. (hereinafter referred to as Kaisha) (European Patent No: EP 0981223 A2).(Publication data: 02/23/2000)

7. **As per claims 1,16and 19,** Ohki discloses the method/apparatus/or a software product for countering unauthorized decryption comprises a step of scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing. [column 2, lines 38-48; column 3, lines 1-19; column 3, line 62-column 4, line13;column 8, line 60-67; abstract; column 7, lines 12-14; column 13, lines 15-21] (As explained on column 13, lines 15-21, for example, the following is recited, In this embodiment, the order of data processes is randomized, a dummy process is added, and the normal data and bit inverted data are used. It is therefore possible to make it difficult to presume the dependency of current consumed by the IC card chip upon data process and to presume the cipher key/decryption key by measuring the wave shape of the consumption current and this meets the limitation of the claims)

8. **As per claims 1-4,16-20** , Kaisha discloses the method/apparatus/or a software product for countering unauthorized decryption comprises a step of scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing.[column 1, ref. Num "0008", ref. Num "0009" and abstract.]

9. **As per claim 2 ,17 and 20 Ohki** discloses the method/apparatus/ or a software product as applied to claim 1 above. Furthermore, Ohki discloses the method wherein the hardware operational phenomenon is power consummated by the hardware to execute the data decryption processing.[abstract; column 7, lines 12-14; column 13, lines 15-21] (As explained on column 13, lines 15-21, for example, the following is recited, In this embodiment, the order of data processes is randomized, a dummy process is added, and the normal data and bit inverted data are used. It is therefore possible to make it difficult to **presume the dependency of current consumed by the IC card chip upon data process and to presume the cipher key/decryption key by measuring the wave shape of the consumption current and** this meets the limitation of the claims)

10. **As per claim 3 and 18 Ohki** discloses the method/apparatus/ or a software product as applied to claim 1 above. Furthermore, Ohki discloses the method wherein the hardware is a IC card, a PDA, or a cellular phone.[Abstract] (The data process order is randomly exchange and this will reduce the dependency of consumption current of **an IC chip** upon the data process.)

11. **As per claim 4, Ohki** discloses the method/apparatus/ or a software product as applied to claim 1 above. Furthermore, Ohki discloses the method wherein the data decryption processing is executed to decrypt data encrypted by a RSA encryption processing or an elliptic encryption processing.[Column 13, lines 22-27; column 14, lines 63-66]

Allowable Subject Matter

12. **Claims 5-15 objected** to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
05/09/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100